# Cranbrook Church of England Primary School

# Information Acceptable Use Policy

| | |
|---|---|
| **Written by: Rosie Piper/ KCC** | March 2018 |
| **Agreed by governors:** | May 2018 |
| **To be reviewed:** | March 2019 |

| | |
|---|---|
| **Signed by Chair of Governors:** | |
| **Signed by Headteacher:** | |

# Information Acceptable Use Policy

At Cranbrook C of E Primary School we are committed to ensuring that use of the internet and other technologies is used to enhance learning and ensure pupils are prepared for the world we live in. However, we are aware that with the opportunities brought by the internet and associated technologies, there are associated risks. This policy contains the pupil, parent/ carer, staff and volunteer acceptable use agreements. Staff and volunteers agree to these statements on induction and this is redistributed whenever changes are made to the policy. Pupils have these statements discussed with them through computing and e-safety lessons, and reminders are displayed in the computing suite in the form of posters. This policy should be read in conjunction with our e-safety policy.

This policy sets out a code of conduct within the usage agreements, which is required to be signed by all users who wish to use the computer system at Cranbrook Church Of England Primary School. It outlines clearly the need for responsible usage of the computer system.

The computer system and network (henceforth referred to as the "system") is owned by Cranbrook Church Of England Primary School, and may be used by students to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The Acceptable Usage Policy has been drawn up to protect all parties - the pupils, the staff, the guests (henceforth referred to as the "user(s)") and Cranbrook Church Of England Primary School.

The school reserves the right to examine or delete any files that may be held on its system or to monitor any Internet sites visited.

Users requesting access to the system and internet should sign a copy of this Acceptable Usage Policy and return it to the Headteacher for approval.

*Acceptable Usage:*

## Access

- The system may not be used for private purposes, unless the headteacher has given permission for that use, and it does not contravene any rule below.
- Access should only be made via the user's own authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the system, or activity that attacks or corrupts other systems, is forbidden and will result in the user's access being removed.
- The system's security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

## Software

- That all users are aware of the legal responsibility of using only licensed software on any system.
- That users are aware that unauthorised software copies may contain viruses, which could affect the integrity of the whole system, and that unauthorised software are not allowed to be used on any workstation.

- That any software downloaded from the internet, or contained on CD ROMS/USB Storage Devices received through the post or magazines are not be loaded without the prior permission of the Headteacher.
- Users are not permitted to copy any software application from the computer system to use outside of the business.

## Schools Information Management System (SIMS)

- Be aware of the Data Protection Act. Information that is stored in this system is private and confidential and should only be shared with parties that it concerns.
- Only place information within a person's record that a user with a legal responsibility for that person has a right to see.
- Users must not distribute or disclose any information obtained from the system to any person(s) with the exception of those to which the information relates, or to another entity with legal responsibility for that person.

## Anti-Virus Software

- The system automatically virus-checks data files which are added via email attachments and removable storage devices (i.e. CD ROM, USB drives, etc.). The Anti-Virus software will aim to prevent access to or remove any unwanted files or applications if a virus is found.

  This procedure is overseen by the ICT technician. If a virus is detected, the user will be notified with an error message, please see the ICT support team for assistance in dealing with infected files.
- Anti-Virus software should not be overridden or turned off at any time.

## Data Transfer

- That any transfer of data from home computer to the system, is only attempted after virus checking.
- On being made aware that a file is infected with a virus, the user should inform the ICT technician.
- Any data containing personal details (including photographs of children), should not be taken off-site, stored on personal removable media, or sent to personal email addresses, etc.
- Use of cloud services to store data (i.e. DropBox, Google Drive, Box, etc.) from the system is forbidden. These services are not fully compliant with the Data Protection Act.

## Internet

- All Internet activity should be appropriate to the user's professional activity or education.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Use of chat rooms, dating, and social media websites are not allowed.
- Use of websites or applications to circumvent the business web filtering in order to access blocked websites is forbidden.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

## E-mail

- Users are responsible for all E-mail sent, and for contacts made that may result in E-mail being received.
- E-mail should be written carefully and politely, particularly as messages may be forwarded, inadvertently be sent to the wrong person or printed and be seen by unexpected readers.
- E-mail should be used for business use. Personal use of the e-mail system is forbidden. Business owned e-mail address may not be used for signing up to social networking/media sites, shopping sites, personal banking or other sites unrelated to the business.
- E-mail may be pushed to mobile devices. These devices will be required to have a passcode.
- E-mail access should not be via any third-party company, software or application.

## Printing

- Printing is to be used for business purposes only.
- Some printers are automatically set to double-sided (duplex) to save paper.
- Colour printing should only be used for final copies of documents.

## Bring Your Own Device (BYOD)

- Users are responsible for their own devices and use them at their own risk. The business is not responsible for any damage, lost, or theft of personal devices used on site.
- Users wishing to use their own device should ensure it has appropriate up to date anti-virus software installed.
- Internet access on personal devices is filtered in the same manner as using the business' own devices, and will require the user to login with their network credentials in order to access the internet.
- Configuration of the device for using Wi-Fi to access the internet can be provided by the ICT Support Team. The business accepts no liability when configuring the device for use on the business network; repair or upgrade of a device is the owner's responsibility, and will not be undertaken by the ICT Support Team.

## Storage

- Users are provided an area on the system in which to save their work which will be backed up by the ICT Support Team on a regular basis, storage of personal items are not permitted.
- Storing digital copies of films on the system are not permitted unless the ICT Support Team have put them on the system and are in accordance with the licence with which they were purchased.
- Storing digital music collections on the system are not permitted unless the ICT Support Team have put them on the system and are in accordance with the licence with which they were purchased.

## Equipment

- All equipment owned by the business is security marked, and any devices that are mobile are assigned to a user that is responsible for that device.
- Users are responsible for the equipment that they use. A record of user access to the device is kept and any damage to equipment will result in a cost incurred to the user for repair or replacement where necessary.
- Any equipment that is loaned to a user must be returned either when leaving the business or on request.
- Staff are responsible for the computer equipment in the room for each lesson, and will check all devices are working correctly and without damage, at the start and end of every lesson.

## Irresponsible use

Users are liable for any potential misuse of the system and/or breach of the Data Protection Act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

- The business reserves the right to revoke or deny access to the system where a user or users are found to be in breach of this policy.

*Procedure:*

Each user will be asked to sign this Information Systems Acceptable Usage Policy before gaining access to the school computer network. The signed document will be kept on file for each employee or student.

Please complete the following in BLOCK CAPTIALS, sign and returned.

**Full Name:** .....

**Position in school:** .....

**Signature:** ..... **Date:** .....

**For ICT Support Team use:**

**Access granted:** ..... **Date:** .....

| Pupils Acceptable Use Policy |
| --- |
| |
| Statements for Early Years and KS1 (0-7)<br>• I only use the internet when an adult is with me<br>• I only click on links and buttons when I know what they do<br>• I keep my personal information and passwords safe online<br>• I only send messages online which are polite and friendly<br>• I know the school can see what I am doing online<br>• I know that if I do not follow the rules then:<br>  ◦ I will move down the class behaviour rocket<br>• I always tell an adult/teacher if something online makes me feel unhappy or worried<br>• I can visit www.thinkuknow.co.uk to learn more about keeping safe online<br><br>EYFS and KS1 shortened version (for use on posters)<br><br>• I only go online with a grown up<br>• I am kind online<br>• I keep information about me safe online<br>• I tell a grown up if something online makes me unhappy or worried |
| Statements for KS2 Pupils (7-11)<br>• I always ask permission from an adult before using the internet<br>• I only use websites and search engines that my teacher has chosen<br>• I use my school computers for school work unless I have permission otherwise<br>• I ask my teacher before using my own personal devices<br>• I know that if I have brought a mobile phone to school, this has to be handed into the office at the start of the day<br>• I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult<br>• I only talk with and open messages from people I know and I only click on links if I know they are safe<br>• I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened<br>• I only send messages which are polite and friendly<br>• I keep my personal information safe and private online<br>• I will keep my passwords safe and not share them with anyone<br>• I will not access or change other people's files or information<br>• I will only post pictures or videos on the Internet if they are appropriate and if I have permission<br>• I will only change the settings on the computer if a teacher/technician has allowed me to<br>• I understand that the school's internet filter is there to protect me, and I will not try to bypass it.<br>• I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult<br>• I know that my use of school computers and Internet access will be monitored<br>• I know that if I do not follow the rules then:<br>  ◦ I will lose one or more Dojo points, which may result in a detention<br>• If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away<br>• If I am aware of anyone being unsafe with technology then I will report it to a teacher |

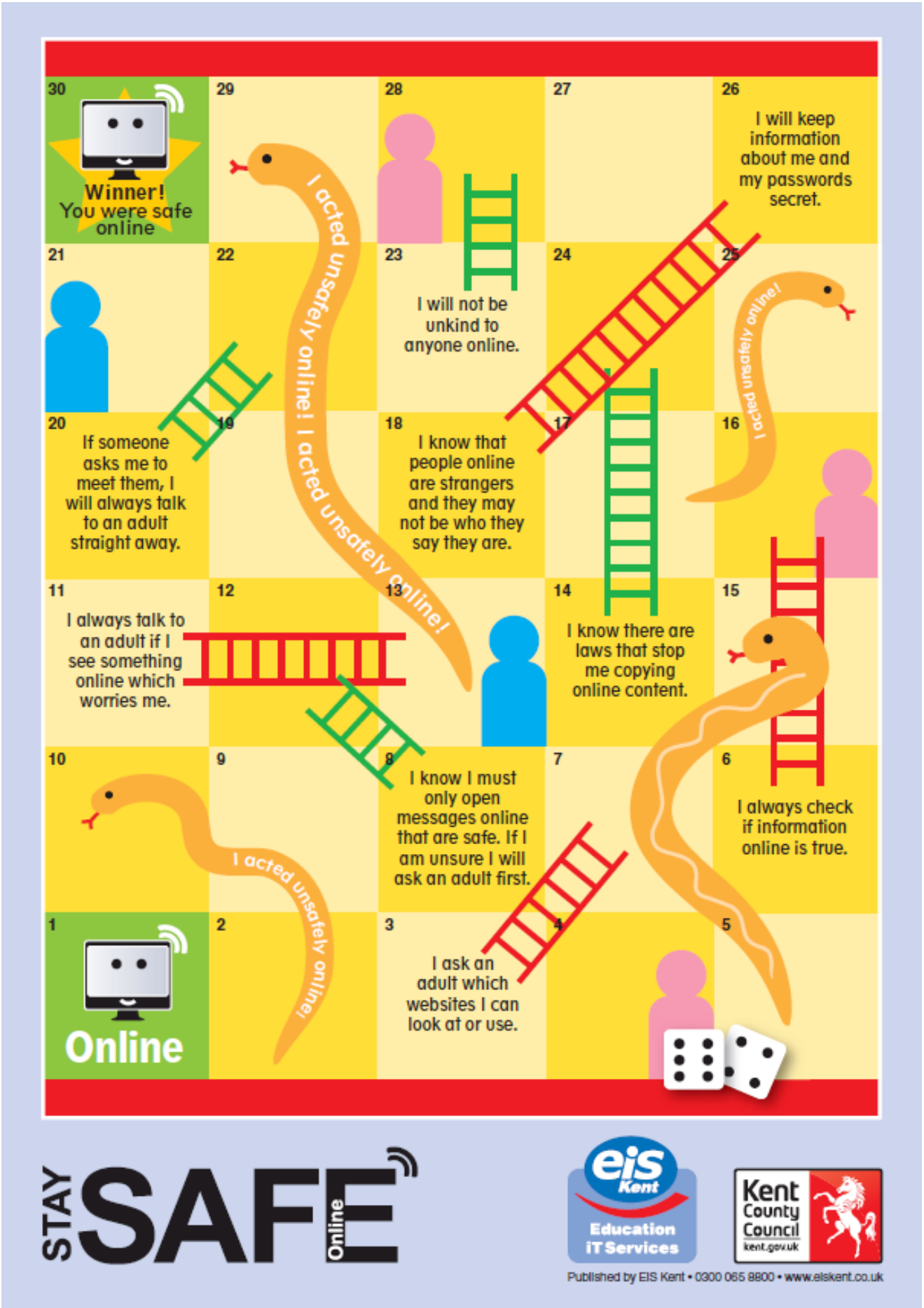
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online

KS2 Shortened version (for use on posters)

- I ask an adult which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe and if I'm unsure then I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up then I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried


Be
SAFE
Online
1 I only go online with a grown up
2 I am kind online
3 I keep information about me safe
4 I tell a grown up if something online makes me unhappy
???
eis Kent
Education IT Services
Kent County Council
kent.gov.uk
Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

# KS2 Acceptable Use Poster



# Parent/Carers Acceptable Use Policy Statements

- I have read and discussed the Acceptable Use Policy (attached) with my child
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
- I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the schools behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-Safety) and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I know that I can speak to the school Online Safety (e-Safety) Coordinator (Rosie Piper), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)
- I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site will be stored on an encrypted USB stick approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including files, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will protect the devices in my care from unapproved access or theft. I will not under any circumstances take photos or videos on my personal devices.

8. When/ if accessing secure internet sites from personal devices (e.g. assessment system) I will not have my username or password saved to my device.

9. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

10. I will respect copyright and intellectual property rights.

11. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead/ the E-safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to one of the Designated Safeguarding Leads as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider (or School Business Manager in their absence) as soon as possible.

13. My electronic communications with pupils and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with one of the Designated Safeguarding Officers and/or or the Head Teacher.

18. In accordance with the school's e-safety policy, I understand that personal mobile phones should not be used within the classroom/ areas where pupils are present, without express permission from the headteacher, for a specific purpose. I will not use personal devices, such as mobile phones, to take photos or videos of pupils and will only use work-provided equipment for this purpose. I acknowledge that I am not permitted to use my personal phones or devices for contacting children or their families within or outside of school in a professional capacity, other than on school trips or events in an emergency.

19. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

    *The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.*

# Visitor/Volunteer Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I have received an induction outlining the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

2. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

3. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

4. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

5. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

6. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead or the Head Teacher.

7. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Rosie Piper) as soon as possible.

# Social Networking Acceptable Use Policy

*For parents/volunteers running school/setting social media accounts e.g. PTA groups*

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety). I am aware that Facebook is a public and global communication tool and that any content posted on the site/page/group may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the head teacher. The head teacher (or other appropriate member of senior leadership) retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of the Facebook page or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. Images of pupils will be taken on school equipment by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school and these will be for the sole purpose of inclusion on Facebook and will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of Facebook and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

6. I will set up a specific account/profile to administrate the site (unless acting as myself as a class representative, rather than on behalf of the school) and I will use a strong password to secure the account. If acting on behalf of the school (e.g. School PTA) the school Designated Safeguarding Lead and/or school management team will have full admin rights to the account.

7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher immediately.

9. I will ensure that the Facebook page is moderated on a regular basis as agreed with the head teacher.

10. I have read and understood the school Online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

11. If I have any queries or questions regarding safe and acceptable practice online I will raise them with the headteacher.